Cooley

The First Trump Cybersecurity Executive Order

May 18, 2017

On May 11, 2017, less than four months after his inauguration, President Trump signed a long-anticipated Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (hereinafter, the "EO"). The EO clearly shows we live in very different times and very different circumstances than the Obama administration, which (for a variety of reasons) didn't pass its initial cybersecurity executive order until four years in.

Because of its nature, the EO focuses on the security of the federal government's current IT infrastructure, protections against cyber threats facing critical US infrastructure and goals for international cooperation and workforce education with respect to cybersecurity. We have seen other cybersecurity executive orders, however, whose effects have spilled over into the commercial sector. For example, Executive Order 13636 – that was mentioned above and signed by Obama in 2013 – established the NIST Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"). That Framework has been adopted on a much wider basis, including amongst commercial corporate entities. Some commentators have noted that various aspects of the Trump cyber EO similarly could be informally extended well beyond the government.

Cybersecurity of federal networks

The first and lengthiest section of the EO mandates steps to improve the federal government's cybersecurity practices and information technology infrastructure, noting that the government "has for too long accepted antiquated and difficult-to-defend IT." It provides that, going forward, agency heads will be held accountable for their agencies' risk management processes. The EO also requires agencies to implement the Framework (and any successor documents) to manage cybersecurity risk, effective immediately. Agency heads will be required to provide a risk management report within 90 days following the date of the EO describing the agency's plan for implementing the Framework. In addition, the EO tasks the Director of the American Technology Council with compiling a report to the President recommending ways in which to modernize and secure federal IT services.

Cybersecurity of critical infrastructure

The EO's second section addresses federal support for critical infrastructure owners and operators. Specifically, the EO directs agency heads to work with, and identify capabilities such agencies can employ to support, "the cybersecurity efforts of critical infrastructure entities … at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." In particular, the EO calls out threats from botnet attacks, electricity disruptions and prolonged power outages resulting from cyber incidents and cybersecurity risks facing the military's industrial base and supply chain. In addition, the EO requires agency heads to examine the sufficiency of current federal policies promoting market transparency of such critical infrastructure entities' cybersecurity risk management practices, focusing on public companies in particular.

Cybersecurity for the nation

Third, the EO sets priorities for national cybersecurity policy, chief among them to "promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft." To advance the goals of deterrence and protection, several agency heads are tasked with reporting on the nation's strategic options for protecting against and deterring cyber threats. In addition, relevant agency heads will be required to provide reports on their international cybersecurity priorities, including with respect to investigation, cooperation and sharing information regarding cyber threats, following which the Secretary of State will provide a report to the President setting forth an international cybersecurity engagement and cooperation strategy.

Workforce modernization

Finally, the EO addresses the country's need to develop and maintain a cybersecurity-trained workforce "to ensure that the United States maintains a long-term cybersecurity advantage." To that end, the EO requires several agency heads to assess and provide the President with reports regarding the "scope and sufficiency" of current efforts to educate and train American workers in cybersecurity through education curricula and apprenticeship programs, as well as similar workforce development practices of foreign nations.

What the EO means to you

Cybersecurity is a nonpartisan issue, so despite the current political climate, one would not expect much negative reaction to the EO. Not only has there been little negative reaction, there has actually been a somewhat surprising amount of positive reaction from a wide variety of stakeholders. For a variety of reasons, from the notion of accountability, to the action-based next steps, to the embracing of the Framework, most people have (so far) been guardedly optimistic. For private companies, this means that the various efforts called out in the EO could filter down to those private enterprises.

Cooley has significant expertise in both cybersecurity generally and with the Framework specifically. Our privacy & data protection practice is consistently designated as one of the best in the country. Please feel free to reach out to contact any of the identified attorneys on this alert for more information or assistance in responding to the EO.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Matthew D. Brown **San Francisco**	**brownmd@cooley.com** **+1 415 693 2188**
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.